Privacy Impact Assessment
for the

Automated Passport Control (APC) and Mobile Passport Control (MPC)

DHS/CBP/PIA-051

March 19, 2018

Contact Point
John Maulella
Office of Field Operations
U.S. Customs and Border Protection
(202) 344-2605

Reviewing Official
Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The U.S. Department of Homeland Security (DHS) U.S. Customs and Border Protection (CBP) developed the Automated Passport Control (APC) and Mobile Passport Control (MPC) programs to automate and expedite eligible travelers' entry process into the United States. These programs enable travelers to perform select entry declaration and inspection requirements tasks through a self-service kiosk (APC) or a mobile device application (MPC). DHS is conducting this Privacy Impact Assessment because APC and MPC collect personally identifiable information (PII) from members of the public.

Introduction

CBP is charged with protecting U.S. borders while facilitating lawful travel and trade. The growing volume of travelers and trade entering the United States increases demands on the limited resources of CBP. Advances in technology, such as automated kiosks and mobile applications, provide alternative approaches that allow CBP to optimize limited officer resources. These technological advances also assist airport authorities in facilitating traveler entry processing and reducing wait times. As part of this effort, CBP developed a set of application programming interfaces known as APC Services, which enables authorized devices to collect biographic and inspection-related information from travelers. APC Services validates this data and securely transmits it to other federal systems[1] to query for derogatory information. APC Services reduces the administrative burden on U.S. Customs and Border Protection Officers (CBPO), allows for a more intelligent queuing process, and provides for a more efficient entry process for travelers. Ultimately, the use of these technologies helps reduce inspection time and overall wait times for the traveler while allowing CBPOs to focus on the inspection and other related border security responsibilities. APC Services uses two types of devices to collect information: (1) Automated Passport Control (APC) and (2) Mobile Passport Control (MPC).

[1] Includes the below systems. Privacy Impact Assessments and System of Records Notices for the DHS systems can be found at https://www.dhs.gov/privacy.

- National Crime Information Center (NCIC), via a CBP interface (all travelers) – for more information about the FBI's NCIC, please *see* https://www.fbi.gov/services/cjis/ncic.
- DHS Office of Biometric Identity Management (OBIM), Automated Biometric Identification System (IDENT) system (Foreign travelers aged 14 to 79, except Canadian Passport and Canadian Lawful Permanent Resident travelers);
- CBP Advance Passenger Information System (APIS), flight manifest data (all travelers);
- CBP TECS, Primary Query System (PQS) vetting (all travelers);
- CBP TECS, Travel Document and Enforcement Data (TDED) system (all U.S. documents);
- CBP Electronic System for Travel Authorization (ESTA) (Visa Waiver travelers); and
- CBP Electronic Visa Update System (EVUS) (Chinese 10-Year Visa travelers);
- CBP Automated Targeting System (ATS), vetting (all travelers).

Automated Passport Control (APC)

APC uses free-standing, self-service kiosks to expedite the CBP entry process for eligible travelers, to include U.S. citizens, Canadian visitors, U.S. Lawful Permanent Residents (LPR), Visa Waiver Program (VWP) participants entering under the waiver-business (WB) or waiver-tourist (WT) class of admission,[2] and other non-immigrants.[3] These kiosks, which are purchased by either terminal operators, airports, or seaport authorities, are installed at select airports and seaports and are maintained by one of several approved vendors to help decrease wait and inspection times. Eligible travelers submit biographic information and responses to inspection-related questions, prior to inspection by a CBPO. Previously, a CBPO inspected travelers and asked them questions in order to verify the purpose and intent of travel. Vendor-maintained APC kiosk systems use APC Services to transmit biographic information and responses to inspection-related questions to CBP systems and other federal information technology systems for vetting purposes.[4] Use of the kiosk is free, voluntary, and does not require membership. APC kiosk systems may not retain PII, including biographic and biometric data. APC Services retains PII via log records for no longer than 30 days. The TECS system, which receives the data via APC Services, retains the biographic information in accordance with the retention schedules outlined in the System of Records Notices (SORN) for TECS[5] and Border Crossing Information (BCI).[6]

Biometric Submission via APC

APC kiosks collect facial images from all travelers and fingerprints from VWP, U.S. visa, and non-Canadian LPR travelers. The kiosk captures a photo and then prints out a receipt with the traveler's face and biographic information. This process allows CBPOs to make one-to-one comparisons of the newly-captured facial images with the travelers themselves. APC facilitates identity verification and law enforcement checks by collecting the following information from the traveler: (1) biographic information including passport information (full name, date of birth, citizenship, passport number, country of issuance, and expiration date), which is transmitted to APC Services in order to query law enforcement databases for derogatory information and confirm that the traveler is listed on the flight's manifest; (2) a facial image in order to provide the traveler with a paper receipt; and (3) fingerprints, when applicable. APC and MPC do not require travelers who are either U.S. citizens or Canadian B1/B2 visa travelers to submit fingerprints. For other travelers, however, the kiosk system collects and submits biometric data to APC Services, where

[2] Participation in VWP requires enrollment in CBP's Electronic System for Travel Authorization (ESTA) program.
[3] Other non-immigrants include U.S. visa holders entering under the following classes of admission: B1/B2, C1/D, and D1.
[4] Includes external systems such as NCIC and DHS OBIM's IDENT, and CBP systems such as TECS (PQS and TDED), APIS, ESTA, ATS, and EVUS.
[5] DHS/CBP-011 U.S. Customs and Border Protection TECS, 73 FR 77778 (December 19, 2008).
[6] DHS/CBP-007 Border Crossing Information, 81 FR 4040 (January 25, 2016).

the data is retained in log records for up to 30 days. Biographic data for all travelers is submitted to APC Services, and retained in log records for up to 30 days.

When travelers approach the APC kiosk, they must acknowledge the CBP Privacy Policy and other required notices[7] by following the instructions provided on the kiosk screen. Then the traveler scans or swipes his or her passport's machine-readable zone (MRZ), poses for a facial photograph captured by the kiosk and its server, and verifies biographic and flight information by answering a series of CBP inspection-related questions on the touch screen. Non-U.S. citizen APC kiosk users must also select a class of admission.

Vetting Process

Upon traveler identification, APC Services conducts traveler vetting, which queries a number of federal systems (listed above) for that particular traveler. Based on the vetting results, APC Services responds to the kiosk with a receipt, either granting passage or requiring additional inspection. For travelers who are referred for further inspection, a referral code will be printed on their receipt, such as referrals for enforcement purposes, biometric failures, or merchandise declarations, to enable the CBPO to more efficiently complete their processing. Next, travelers present their receipts to the CBPO for document verification and inspection-related questions as required to finalize their inspection for entry into the United States. APC receipts are collected and retained in accordance with the disposition policy established for the Customs Declaration 6059B forms.[8]

CBP officially launched the APC program at Vancouver International Airport in May 2013. Since its inception, the program has expanded to CBP operations at more than 50 international ports of entry with future expansions expected. Interested airports can opt to install kiosks in their Federal Inspection Services (FIS) or preclearance areas. The kiosks are provided, maintained, and owned by the airport authority's terminal operator, but approved and installed kiosks must comply with CBP APC technology and business requirements. Based on the agreements with the kiosk vendors, all photos and fingerprints, as well as the associated biographic data, should be purged by the APC kiosk and any associated vendor systems after each transaction, regardless of citizenship or admissibility.[9] However, while biometric data that may be captured from U.S. citizens and Canadian B1/B2 visas is not returned to APC Services, biographic data, photos, and fingerprints from all other travelers are required to be transmitted to APC Services and may be

[7] Notices include Intellectual Property Rights, Paperwork Reduction Act, and Section 311 of the Trade Facilitation and Trade Enforcement Act of 2015 Notice.
[8] Instead of completing a paper Customs Declarations (6059B) form, eligible travelers may proceed directly to an APC kiosk in the passport control area of the airport. If the receipt is free of declarations, it is retained for only three (3) years; however, if the receipt contains dutiable declarations, it is retained for six (6) years.
[9] The Interface Control Document (ICD) governs the interface specifications between the vendor-owned kiosk system and CBP. The ICD states the following, "The Kiosk System shall not store any privacy-sensitive data such as MRZ data, personal traveler data, or referral codes."

retained in log data for up to 30 days.

Mobile Passport Control (MPC)

Much like APC, MPC is the product of a public-private partnership in which CBP partners voluntarily elect to participate. With MPC, U.S. citizens, Canadian visitors, and, in some cases, VWP participants may use an approved mobile application loaded onto their personal smartphone or tablet to expedite the entry process into the United States. Similar to APC, MPC improves processing times by allowing eligible travelers and their families to submit passport information and responses to inspection questions, prior to a CBPO inspection. Additionally, MPC-enabled mobile applications, which do not require memberships, are voluntary and free to the user.

In general, MPC-enabled mobile applications can take one of two forms: (1) a standalone application dedicated to the execution of MPC transactions, such as the Airports Council International-North America's (ACI-NA) sponsored application; or (2) an integrated MPC component to a preexisting travel-related mobile application, such as the Miami International Airport's sponsored application. A list of approved MPC-enabled mobile applications is included in Appendix B.

Eligible travelers with a smartphone or tablet may voluntarily download MPC-enabled mobile applications from a mobile application store (*e.g.*, Apple App Store or Google Play Store). Within the mobile application stores, travelers can review the application owner and CBP privacy policies. Following the download but prior to the creation of an MPC profile, the traveler is presented with a list of required CBP notices. Following the traveler's acknowledgement of the notices[10] and his or her affirmative express consent, the traveler creates an MPC profile using his or her passport information. The profile, which can be set up at any time prior to travel, includes the traveler's first and last name, gender, date of birth, passport number, passport expiration, passport country issuing authority, country of citizenship, and a facial photo (*i.e.*, a "selfie"). Once a profile is created, it is securely stored on the phone; there is no option for the user to submit the profile itself to CBP. When the traveler lands in the United States, he or she completes the "New Trip" section within the mobile application by selecting his or her arrival airport and airline, and answers a set of CBP inspection-related questions. After the traveler reviews a summary of his or her responses and certifies that the information is truthful and correct, he or she securely submits the information.

Once the traveler submits the MPC "trip," which includes the traveler's biographic information, inspection question responses, and class of admission (if applicable),[11] the mobile

[10] Notices include Intellectual Property Rights, Paperwork Reduction Act, and Section 311 of the Trade Facilitation and Trade Enforcement Act of 2015 Notice.

[11] While the biographic information, inspection question responses, and class of admission are electronically submitted to CBP, the photo (*i.e.*, "selfie") is never submitted. The photo is only physically shown to the CBPO at

application developer's servers transmit the information to CBP's APC Services for vetting. APC Services encodes and encrypts the vetting results and transmits them back to the traveler's MPC-enabled mobile application in the form of an encrypted Quick Response (QR) code on the electronic receipt, along with other MPC-required biographic information. This QR code indicates that the traveler is either being granted passage or referred. Travelers present their travel documents and MPC electronic receipt (which includes the "selfie" picture) to the CBPO to finalize their inspection for entry into the United States. The CBPO directs the traveler to scan the QR code on a barcode scanner. As a result, the authenticity of the receipt is verified through decryption and display of the encoded information to the CBPO. Travelers receiving a referral code (*e.g.*, declaration, enforcement, technical, or random) will be directed to a triage booth or podium for further inspection or be allowed to enter into the United States. Regardless of the vetting result, the CBPO completes the inspection and verifies the traveler's purpose and intent. MPC eligibility is currently limited to travelers from the United States and Canada but may be expanded to other travelers in the future.

Each of these applications is owned, developed, and maintained by the business sponsors (or one of their private sector partners) and may serve multiple purposes. For example, the application may also provide information on local weather, flight status, or airport information. In these cases, the MPC-enabled mobile application may only notify and require affirmative express consent from the traveler on application permissions and entitlements related to MPC. The traveler is encouraged to carefully read the business sponsor and developer's privacy policy prior to download. Mobile applications may also be integrated with third-party advertisement networks and connected with internet protocol (IP) addresses in foreign countries. The MPC business requirements strictly forbid the business sponsor or application developer from sharing any PII collected by the application for the purposes of MPC with third-party advertisement networks or any other IP addresses not affiliated with CBP (or one of its approved vendors).

All MPC-enabled mobile applications will require access or usage of the following information or device components from the traveler's device: (1) the camera sensor and photo library;[12] (2) read and write external storage; (3) a unique device identifier to authenticate the application with the developer's application servers; and (4) network access. The developer may elect to include other features to improve the traveler's experience. These features are included at the discretion of the developer and are not found within the business requirements. However, for the features that are used for CBP's purposes and are deemed necessary for travel, CBP reviews the use of those features and approves them. Appendix A provides a full description of the CBP

the time of inspection to ensure the traveler associated with the MPC account is the person who is presenting himself/herself for inspection.

[12] Access to the camera/video library is only required so that the traveler can capture the "selfie" and upload it for presentation to a CBPO. The picture is not submitted to CBP.

review process for MPC-enabled mobile applications.

Business sponsors and their application developers may elect to integrate with social media platforms (*e.g.*, Facebook, Instagram, and Twitter) for their own purposes. However, integration with social media is not an MPC business requirement and cannot occur within the CBP process or on an MPC-related screen. Furthermore, no information collected for the purposes of MPC can be shared with third parties for other purposes (*e.g.*, social media, advertising networks). MPC-enabled mobile applications cannot maintain or store CBP records. Travelers have the option of securely storing their MPC profile (and that of their traveling family members) on their own device. The MPC profile may be deleted by the traveler at any time.

CBP officially launched the MPC pilot program at Hartsfield-Jackson Atlanta International Airport on August 13, 2014, and the program expanded to 24 airports and one seaport by early 2018. A full list of approved MPC applications can be found in Appendix B. CBP has released the MPC business requirements, is continuing deployments at additional ports of entry, and is still onboarding new business sponsors (and their application developers).

APC Services

In order to facilitate the operation of APC kiosks and MPC-enabled applications, CBP has developed APC Services, a suite of application programming interfaces that allow authorized APC and MPC devices to collect biographic, inspection-related information and, where applicable, biometric data from travelers. Once the information is transmitted from the kiosk system or MPC-enabled application, APC Services validates the data and, in order to conduct searches for derogatory information, securely shares the applicable traveler data with federal information technology systems for vetting.[13] The use of APC Services during the entry process eases inspection times and wait times for travelers and, as a result, reduces the administrative burden on CBPOs, allowing them to focus on the inspection and other essential border security responsibilities. Specifically, APC Services receives biometric data for VWP travelers, travelers with a U.S. visa, and non-Canadian LPR travelers. For travelers who are admitted into the United States, APC Services creates a record of entry in the TECS system.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974 articulates concepts of how the Federal Government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information. The Homeland Security Act of 2002, Section 222(2), states that the Chief Privacy Officer shall assure

[13] Includes external systems such as NCIC and DHS OBIM's IDENT, and CBP systems such as TECS (PQS and TDED), APIS, ESTA, and EVUS.

that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS. The FIPPs account for the nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure.

DHS conducts Privacy Impact Assessments on both programs and information technology systems, pursuant to the E-Government Act of 2002, Section 208 and the Homeland Security Act of 2002, Section 222. Given that MPC is a program rather than a particular information technology system, this PIA is conducted as it relates to the DHS construct of the Fair Information Principles. This PIA examines the privacy impact of MPC operations as it relates to the Fair Information Principles.

1. Principle of Transparency

Principle: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate. There should be no system the existence of which is a secret.

Eligible travelers who voluntarily elect to use the APC kiosks or an MPC-enabled mobile application must acknowledge a CBP Privacy Policy, a Disclaimer Notice, and the business sponsor and/or application developer's Privacy Policy prior to download. Eligible travelers obtain immediate notice on the kiosk or mobile application screens prior to entering their information. Upon first use of the mobile application, or before the individual provides information, he or she is confronted with a pop-up message that requires his or her direct and affirmative consent in order to continue using the application. The notices inform travelers that the use of these approaches is purely voluntary and that they retain the option of proceeding directly to the CBPO for the more traditional examination. CBP conducts a rigorous review and approval process, which includes a thorough security review, prior to deploying any new mobile application. Appendix A provides a description of CBP's review process.

Before any MPC-enabled application is published to an app store, the business sponsor and the vendor are required to execute an MPC license agreement, which protects the CBP branding and IP address as well as MPC business and security requirements. The license agreement authorizes developers to use the CBP logo and trademark names. CBP conducts compliance testing at least annually and upon every new version release. In the event of noncompliance, CBP may take corrective actions, including a suspension of the application's functionality. CBP has trademarked "Mobile Passport Control" and "MPC." Developers are prohibited from using the

logo without CBP approval.

In addition to the privacy notices described above, CBP provides notice of the APC kiosks and MPC-enabled mobile applications through the publication of this PIA, and provides general notice of its collection of information from travelers entering the United States in the Border Crossing Information (BCI) SORN[14] and TECS SORN.[15]

Privacy Risk: There is a risk that travelers will not receive notice that their biometrics are being collected.

Mitigation: Before travelers enter their information into the APC kiosk or the MPC-enabled application, they are provided with the purpose of the collection and are required to acknowledge the CBP Privacy Policy and other required notices. For both APC and MPC, while biographic data for all travelers is transmitted to APC Services for law enforcement vetting purposes, biometric captures from U.S. citizens and Canadian travelers with B1/B2 visas are not sent to APC Services for retention in CBP systems. For these travelers, biometric captures are purged from the APC kiosk and its server and, for those using MPC, the photos never leave the traveler's phone. However, for all other travelers, biometric data captured by an APC kiosk is transmitted to APC Services, where the data may be retained for up to 30 days.

2. Principle of Individual Participation

Principle: DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

Both APC and MPC rely on information collected directly from the individual traveler, either at the APC kiosk or through the mobile application. APC and MPC collect only similar information to that which has been collected previously through the traditional inspection process. Travelers seeking entry into the United States provide specified personal information in order to facilitate CBP's border inspection and obtain entry into the United States. APC and MPC provide travelers with an alternative approach to providing the required biographic and biometric information to CBP as part of the border inspection process when entering the United States. In order to benefit from these programs, a traveler voluntarily chooses – after being presented with notices that explain that the use is voluntary – to use the kiosk or mobile application in order to transmit his or her PII and answers to the inspection-related questions back to CBP. As an alternative to using APC or MPC, a traveler who prefers not to use the kiosk or mobile application may instead proceed directly to traditional CBP primary examination methods.

[14] DHS/CBP-007 Border Crossing Information, 81 FR 4040 (January 25, 2016).
[15] DHS/CBP-011 U.S. Customs and Border Protection TECS, 73 FR 77778 (December 19, 2008).

Individuals seeking notification of and access to records collected during the process, or seeking to contest their content, may submit a Freedom of Information Act (FOIA) or Privacy Act request to CBP at https://foia.cbp.gov/palMain.aspx, or by mailing a request to:

CBP FOIA Headquarters Office
U.S. Customs and Border Protection
FOIA Division
1300 Pennsylvania Avenue NW, Room 3.3D
Washington, D.C. 20002
Fax Number: (202) 325-1476

Requests for information are evaluated to ensure that the release of information is lawful; will not impede an investigation of an actual or potential criminal, civil, or regulatory violation; and will not reveal the existence of an investigation or investigative interest on the part of DHS or another agency.

All FOIA requests must be in writing and include the requestor's daytime phone number, email address, and as much information as possible of the subject matter to expedite the search process.

Persons who believe they have been adversely impacted by APC or MPC (for example, refused boarding for travel or identified for additional screening by CBP) may submit a redress request through DHS Traveler Redress Inquiry Program (TRIP). DHS TRIP is a single point of contact for persons who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at transportation hubs – like airports, seaports, and train stations or at U.S. land borders. Through DHS TRIP, a traveler can request correction of erroneous data stored in DHS databases through one application. DHS TRIP redress requests can be made online at http://www.dhs.gov/dhs-trip or by mail at:

DHS TRIP
601 South 12th Street, TSA-901
Arlington, VA 20598-6901

Privacy Risk: There is a risk that travelers may not be able to opt-out of using APC or MPC in order to enter the United States.

Mitigation: This risk is mitigated because using APC or MPC is strictly voluntary. Any traveler who does wish to use the kiosk or mobile application may instead choose to use traditional means of primary examination by a CBPO. However, submitting this information to CBP is a requirement of being allowed entry to the United States, whether through APC, MPC, or traditional CBP border inspection process.

3. Principle of Purpose Specification

Principle: DHS should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.

CBP collects travel document data, flight information, appropriate biometric data from the traveler and traveling family members, and declaration information from persons entering the United States, pursuant to the noted authorities under the Immigration and Nationality Act, the Tariff Act of 1930, and other authorities. CBP uses the data to facilitate the entry of legitimate travelers; identify, investigate, apprehend, or remove individuals unlawfully entering the United States; detect fraud or abuse of United States or other nations' passports; and to otherwise enforce U.S. laws at the border. The biographic information, presented by a traveler for admission, will be cross-referenced with data maintained in other law enforcement databases, including the law enforcement data maintained in TECS[16] and the Automated Targeting System (ATS).[17]

CBP's use of the APC kiosk or MPC mobile application does not change the purpose for which the information is collected or the manner in which it is used. The purpose remains consistent with the existing border inspection process. Only the input method of the information has changed.

The following CBP legal authorities allow APC and MPC to collect border crossing information:

- Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Pub. L. 108-458, 118 Stat. 3638;
- Immigration and Nationality Act, as codified at 8 U.S.C. 1185 and 1354;
- Aviation and Transportation Security Act of 2001 (ATSA);
- Enhanced Border Security and Visa Reform Act of 2002; and
- Tariff Act of 1930 as amended, 19 U.S.C. 66, 1433, 1459, 1485, 1624, and 2071.

Privacy Risk: There is a risk that biometric data collected by APC or MPC could be used for another purpose.

Mitigation: This risk is mitigated. CBP uses the data collected via APC and MPC to facilitate the entry of legitimate travelers, to remove individuals unlawfully entering the United States, to detect fraud or abuse of United States or other nations' passports, and to otherwise enforce U.S. laws at the border. While the APC kiosk system transmits biometric data for travelers other than U.S. citizens and Canadian B1/B2 visas to APC Services for up to 30 days of storage in

[16] *See* DHS/CBP/PIA-009(a) TECS System: CBP Primary and Secondary Processing, *available at* https://www.dhs.gov/privacy.
[17] *See* DHS/CBP/PIA-006 Automated Targeting System, *available at* https://www.dhs.gov/privacy.

log data, the APC kiosk system purges all biometric data after the transaction.

Information collected for the purposes of MPC is not retained by the application without the consent of the traveler. The traveler retains the option of storing the profile on his or her device for future travel, or deleting it after use. Ultimately, these photos never leave the traveler's phone. Additionally, although application developers may choose to integrate with social media, this is not an MPC business requirement and cannot occur within the CBP process or on an MPC-related screen. Moreover, information collected for the purposes of MPC cannot be shared with third parties (*e.g.*, social media, advertising networks). CBP applies strict access controls through user passwords, role access, system audits, and employee background checks. These controls help prevent unauthorized access or use.

4. Principle of Data Minimization

Principle: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).

Biographic and biometric information is collected by CBP from all travelers entering the United States in order to confirm the traveler's identity and citizenship, establish whether the traveler is admissible into the United States, and facilitate CBP's enforcement of U.S. laws. APC kiosks and their associated vendor-based system transmit the biographic data of all travelers for law enforcement vetting purposes.

Information collected by the APC kiosk system is not retained by the kiosk (or its owner and vendor). Although photos of U.S. citizens and Canadian B1/B2 visa-holders are deleted by the APC kiosk system, photos of other travelers are transmitted to APC Services and may be retained in log data for no longer than 30 days. The APC kiosk-printed paper receipts are disposed of according to the policy established for the Customs Declaration 6059B forms (*i.e.*, Job Number N1-563-03-3). Specifically, if the receipt is free of declarations, it is retained for three (3) years and destroyed. If the receipt contains dutiable declarations, it is retained for six (6) years and destroyed. MPC-enabled mobile applications, however, allow travelers to voluntarily securely store PII within their MPC profiles on their own device for future travel. At select ports of entry, CBP and the Transportation Security Administration (TSA) have partnered in a program that allows eligible, vetted, low-risk passengers with a connecting flight to receive a second receipt from the APC kiosk. The traveler may present this receipt, which permits one-time expedited access to the TSA Pre-Check lane, to a TSA officer at the checkpoint. The secondary receipt may contain data elements such as the traveler's first name, last name, facial image, flight number, and date/time of travel.[18] TSA expects that as a future alternative, the secondary receipt may be

[18] TSA and CBP stipulate the specific data elements required for the Pre-Check Pass.

leveraged by the MPC-enabled mobile application on the traveler's phone, which is visually presented to a TSA officer in order to access the Pre-Check lane.

This information enables CBP to analyze historical data regarding individuals who cross the border and allows additional DHS components and other government agencies to evaluate their issuance of immigration benefits. Further, it provides DHS and other relevant agencies with the information needed to perform essential enforcement functions.

Consistent with CBP's border security mission and the BCI SORN,[19] border crossing information may be retained for a period of 15 years for U.S. citizens and LPRs, and 75 years for non-immigrant travelers. As mentioned in Principle 3 (Purpose Specification) above, this information, which is presented by a traveler for admission, is cross-referenced with data maintained in other law enforcement databases. As a result, the data shared with TECS is retained for 75 years from the date of collection or for the life of the law enforcement matter, in accordance with the TECS SORN.[20] Similarly, the information shared with ATS is retained pursuant to the source system's retention schedule or for 15 years, whichever is less.

Privacy Risk: There is a risk that U.S. citizens' PII that is collected by APC or MPC may be stored longer than necessary.

Mitigation: This risk is mitigated. Information collected by the MPC-enabled application is not stored by the application. The traveler has the option to store his or her own profile information on a personal device for future travel or may choose to delete it after a single use or at any subsequent point. The APC kiosk system deletes the facial images of U.S. citizens and Canadian B1/B2 visa-holders and does not share them with APC Services.

5. Principle of Use Limitation

Principle: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.

CBP collects travel document data, flight information, biometrics from the traveler and traveling family members, and declaration information from persons seeking to enter the United States to facilitate the entry of legitimate travelers and to apprehend and remove individuals unlawfully entering the nation. Individual DHS users are granted access to border crossing information and TECS enforcement information according to their job role, their need to know, and the mission of their component. CBP will share APC/MPC data within DHS consistent with the terms described in the relevant SORNs listed above. The following DHS components have regular access to border crossing information: U.S. Immigration and Customs Enforcement, U.S.

[19] DHS/CBP-007 Border Crossing Information, 81 FR 4040 (January 25, 2016).
[20] DHS/CBP-011 U.S. Customs and Border Protection TECS, 73 FR 77778 (December 19, 2008).

Citizenship and Immigration Services, TSA, the United States Coast Guard, and the DHS Office of Intelligence and Analysis. In addition, information may be shared with federal, state, local, tribal, international, or foreign governments, or law enforcement agencies to support security activities such as intelligence, counterintelligence, antiterrorism, law enforcement, and threats to national and international security.

Privacy Risk: There is a risk that CBP will use APC or MPC information for a purpose other than those specified for the original collection.

Mitigation: This risk is mitigated. CBP uses the data collected via APC and MPC to facilitate the entry of legitimate travelers, to remove individuals unlawfully entering the United States, to detect fraud or abuse of United States or other nations' passports, and to otherwise enforce U.S. laws at the border. While facial images captured from U.S. citizens and Canadian B1/B2 visas are purged at the APC kiosk system and are not returned to APC Services, photos of other travelers are transmitted to APC Services. CBP shares APC/MPC data but only consistent with the terms described in the relevant SORNs listed above. CBP retains information collected in APC/MPC in accordance with the retention policies described in Principle 4 (Data Minimization) above. CBP also provides notice of this sharing in the relevant SORNs.

Privacy Risk: There are privacy risks associated with the fact that MPC-enabled applications may connect to third-party advertisement networks, which may lead travelers to believe that their information is being used for marketing or other commercial purposes.

Mitigation: This risk is partially mitigated. The CBP Privacy Office will conduct a CBP Privacy Evaluation[21] within one year of publication of this PIA to ensure that the government and commercial partners are in compliance with the required privacy protections. CBP is planning to implement a regular internal audit process by which MPC might be monitored to ensure that no information is used for purposes other than that which was intended for MPC. In addition, CBP's formal agreements and business rules with MPC vendors describe the prohibition against the retention of travelers' PII or its use for commercial or other purposes. MPC is an official trademarked name. The sole purpose of MPC-enabled applications is to use this information only to fulfill CBP's entry declaration and inspection requirements for travelers, as described throughout this PIA.

[21] The results of the CBP Privacy Evaluation will be shared with the DHS Privacy Office.

6. Principle of Data Quality and Integrity

Principle: DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.

Because APC and MPC collect relevant information directly from eligible persons who wish to enter the United States just prior to travel or entry into the country, there is relatively high confidence that the information is accurate and complete. These travelers provide their own information and that of their traveling family members through the APC kiosk or MPC-enabled application prior to encountering a CBPO as part of the border inspection process. Upon arrival, the traveler also answers customs declaration questions for him or herself and traveling family members and provides the data via the kiosk or mobile device to APC Services to facilitate the border inspection process. Because the information is submitted while in flight or upon arrival and the receipt is only valid for four hours, the information is timely.

To ensure accuracy and integrity, the CBPO reviews the information during the inspection process. The CBPO uses the information submitted by the traveler (including responses provided by the traveler directly to the CBPO), the travel document(s) provided, and the CBPO's own observations to conduct the border inspection. If any information appears to be inconsistent, the traveler may be referred for additional processing to clarify or resolve the inconsistency. In addition, vendors providing APC kiosks and MPC-enabled applications must meet certain technology and business requirements. These requirements include certain types of licensing agreements, technical and legal requirements, general layout and process flow rules, branding requirements, prohibitions against certain types of advertising, Privacy Act notices, Paperwork Reduction Act notices, and security and privacy compliance, including proper notice and consent.

Privacy Risk: There is a risk that the traveler will incorrectly enter his or her information into the APC kiosk or MPC-enabled application.

Mitigation: This risk is partially mitigated. Because data entry error is always a possibility, CBPOs are trained to verify and confirm the traveler's information upon inspection. In addition, any traveler may request a correction of his or her inaccurate information through DHS TRIP, which is described in Principle 2 (Individual Participation) above.

7. Principle of Security

Principle: DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

The APC kiosk system and the MPC-enabled application transmit the data directly to APC Services using secure encryption protocols. For instance, no individual can access information on other travelers at the APC kiosk. For the MPC, the traveler retains the option of storing profile information on his or her device for future travel or deleting it after a single use. Transmission of the information via secure electronic transmission reduces the potential for inadvertent exposure of the information to those without a need to know (*i.e.*, unintended or inappropriate disclosure).

As part of the security assessment, DHS information technology professionals analyze the MPC-enabled application to assess the overall security of the application and identify potential vulnerabilities. More specifically, they scan and test the MPC-enabled application to determine the level of security and accessibility, and CBP shares the analysis with the application developer. The application developer is required to address each issue and implement many key recommendations. In addition, the Privacy Policy must notify the user if the MPC-enabled application interacts with certain other active applications on the user's device, such as the camera, which are necessary to effectively operate the application during the entry process. Previously completed security analysis and functional requirements have been incorporated into current and future business requirements.

Sharing within DHS is established on a need to know basis (*i.e.*, employees with a need to know in the performance of their official duties). Toward that end, CBP controls internal access to information through the strict use of controls such as: user passwords, role access, and system audits that track and report access to the data, as well as through employee background checks. These controls help prevent unauthorized access or use within DHS.

As discussed in Principle 5 (Use Limitation), information may also be shared with other domestic and foreign governments, as well as law enforcement agencies with a need to know and in support of the CBP mission. More frequent sharing arrangements usually are established through formal agreements such as Memoranda of Agreement and Memoranda of Understanding. Less frequent sharing is accomplished through written requests for specific information. In both cases, CBP ensures that the recipient implements safeguards to protect the shared information against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure. The specific safeguards and method of information transmission will vary with the requestor and the nature of the request.

Privacy Risk: There is a risk that unauthorized individuals may view the information in APC or MPC.

Mitigation: This risk is mitigated. Information is securely transmitted to and from APC and MPC in adherence with strict encryption protocols. No individual can access information on other travelers at the APC kiosk. This reduces the potential for inadvertent exposure of the information to individuals who do not have a need to know. In addition, CBP ensures that the recipient of shared information implements safeguards to protect the shared information against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure. CBP also applies strict access controls, based on the need to know, through user passwords, role access, employee background checks, and system audits that help prevent unauthorized disclosures. Information relevant to and stored within MPC-enabled mobile applications is also encrypted.

Privacy Risk: CBP collects large amounts of PII in paper form via the APC kiosk receipts, increasing the risk of unauthorized disclosure or access.

Mitigation: This risk is partially mitigated. CBP will be conducting internal audits to confirm that the appropriate privacy and security protections are being implemented by all parties, including vendors for the APC kiosks and MPC-enabled mobile applications. The APC kiosk-printed paper receipts are retained according to the policy established for the Customs Declaration 6059B forms. If the receipt contains dutiable declarations, it is disposed of after six (6) years; however, if it is free of declarations, it is disposed of after three (3) years. Finally each port of entry is developing a standard operating procedure for processing and accepting the APC receipt at the egress point. CBP provides guidance to CBPOs to ensure that the receipts are promptly processed, secured, and disposed of per the port policy.

8. Principle of Accountability and Auditing

Principle: DHS should be accountable for complying with these principles, provide training to all employees and contractors who use PII, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

Internal access to the information provided by travelers during the border crossing is limited to DHS employees and contractors who have successfully completed annual privacy and security training. Access audit logs are reviewed periodically by Office of Internal Affairs. Security requirements for both APC and MPC stipulate that the kiosks and MPC-enabled applications shall not maintain CBP records or user information or otherwise permit use or distribution of CBP or user information unless specifically authorized in writing by CBP. In addition, the business requirements state that the kiosk system and mobile application must allow CBP to review and audit any code, encryptions, network connections, and any other technical specifications.

Privacy Risk: There is a risk to auditing and accountability because CBP cannot dictate security or auditing requirements to the APC or MPC vendors.

Mitigation: This risk is mitigated. CBP will conduct an internal audit during 2018 to confirm that the appropriate privacy and security protections are being implemented by all parties, including vendors for the APC kiosks and MPC-enabled mobile applications. Additionally, the CBP Privacy Office will conduct a CBP Privacy Evaluation[22] within one year of publication of the PIA to ensure that the government and commercial partners are in compliance with the required privacy protections.

Responsible Officials

John Maulella
Director
Admissibility and Passenger Programs
Office of Field Operations

Debra L. Danisek
CBP Privacy Officer
Privacy and Diversity Office
Office of the Commissioner

Approval Signature Page

Original, signed copy on file with the DHS Privacy Office.

_____

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security

[22] The results of the CBP Privacy Evaluation will be shared with the DHS Privacy Office.

APPENDIX A: Mobile Application Security Review Process

Any new CBP MPC-enabled mobile application, prior to deployment, must pass a rigorous approval process, which includes a thorough security review. The application must pass all four tests prior to approval. CBP reevaluates all approved applications at least annually and upon every new major release of the application or change to their Requirements Traceability Matrix (RTM) submission (which includes the network topology):

- **DHS Security (RTM)** – The business sponsor (and its contractors) must provide CBP with a network topology and response to a list of questions related to the physical, management, and IT security requirements for their server sites. This submission must comply with CBP's information system security requirements before approval to participate in the MPC program.
- **MPC Screenshot Compliance Review** – CBP's MPC Program Office must provide the application developer with screen-by-screen feedback in order to fulfill the program's business requirements (which includes privacy requirements such as the display of privacy notices). The developer may repeat these submissions multiple times before approval.
- **Functionality Testing** – The MPC Program Office must provide the application developer with compliance feedback on required functionality that is identified within the program's business requirements. The MPC Program Office uses a test script designed to ensure that the required functionality and notices are given prior to allowing the traveler to perform a given action. For example, one specific test ensures that a "pop-up notification" is presented to the traveler before allowing the application to access a facial image stored on the device or use of the phone's camera. This step can only be executed after being given access to the application developer's beta version of the MPC-enabled mobile application. This step occurs after the Screenshot Compliance Review is approved and must be completed prior to publishing the application into Apple App Store and Google Play Store.
- **DHS Software Assurance Scan** – This step requires CBP's MPC Program Office to coordinate with specified DHS offices to use third-party tools designed to scan the application's coding in order to identify potential vulnerabilities and permissions/entitlements granted to the application upon download. The CBP Information Systems Security Officer (ISSO) reviews this information and provides feedback to the application developer. All CBP-identified vulnerabilities must be remediated and, subsequently, confirmed by a follow-up software assurance scan. If any of the scan's findings (*e.g.*, application-granted permissions and entitlements and IP addresses) are determined to be inconsistent with earlier business sponsor-provided documentation (*e.g.*, RTM, Screenshot Compliance Review, or

Functionality Testing), the application will fail this step. The business sponsor and application developer may resubmit once remediations are made.

APPENDIX B: Approved Mobile Applications

DHS analyzed the MPC-enabled applications below to assess overall security and identify potential vulnerabilities, according the process outlined above. The application developer addressed each reported issue and implemented recommendations. CBP incorporated the final security analysis and the developer's functional requirements into current and future business requirements. CBP approved the following MPC-enabled mobile applications for deployment:

- Airside Mobile, in cooperation with the Airports Council International-North America (ACI-NA), Mobile Passport App
  - Available for both Android and iOS/Apple users
  - Deployed in August 2014
  - Available at the seaport, Port Everglades (PEV), as well as the following 24 U.S. international airports:
    - Hartsfield-Jackson Atlanta International Airport (ATL)
    - Baltimore/Washington International Thurgood Marshall Airport (BWI)
    - Boston Logan International Airport (BOS)
    - Chicago O'Hare International Airport (ORD)
    - Dallas/Fort Worth International Airport (DFW)
    - Denver International Airport (DEN)
    - Fort Lauderdale-Hollywood International Airport (FLL)
    - Houston George Bush Intercontinental Airport (IAH)
    - Los Angeles International Airport (LAX)
    - William P. Hobby Houston International Airport (HOU)
    - Miami International Airport (MIA)
    - Minneapolis-Saint Paul International Airport (MSP)
    - John F. Kennedy International Airport (JFK)
    - Newark Liberty International Airport (EWR)
    - Orlando International Airport (MCO)
    - Phoenix Sky Harbor International Airport (PHX)
    - Raleigh-Durham International Airport (RDU)
    - Sacramento International Airport (SMF)
    - San Diego International Airport (SAN)
    - San Francisco International Airport (SFO)
    - San Jose International Airport (SJC)
    - Seattle-Tacoma International Airport (SEA)
    - Tampa International Airport (TPA)
    - Washington Dulles International Airport (IAD)

- Miami Dade International Airport (MIA), "Airport Official" MPC App

- Available for both Android and iOS/Apple users
- Deployed in August 2017 to MIA